Resilient Control under Denial-of-Service:Robust Design

Feng, Shuai; Tesi, Pietro

Published in:
ArXiv

Publication date:
2016

Resilient Control under Denial-of-Service: Robust Design

Shuai Feng and Pietro Tesi

***Abstract*— In this paper, we study networked control systems in the presence of Denial-of-Service (DoS) attacks, namely attacks that prevent transmissions over the communication network. The control objective is to maximize frequency and duration of the DoS attacks under which closed-loop stability is not destroyed. Analog and digital predictor-based controllers with state resetting are proposed, which achieve the considered control objective for a general class of DoS signals. An example is given to illustrate the proposed solution approach.**

I. Introduction

Owing to advances in computing and communication technologies, recent years witnessed a growing interest towards cyber-physical systems (CPSs), *i.e.*, systems where physical processes are monitored/controlled via embedded computers and networks, possibly with feedback loops that are implemented on wireless platforms [1], [2]. The concept of CPSs is certainly appealing for industrial process automation; however, it raises many theoretical and practical challenges. In particular, the concept of CPSs has triggered considerable attention towards networked control in the presence of cyber attacks. In fact, unlike general-purpose computing systems where attacks limit their impact to the cyber realm, attacks to CPSs can affect the physical world: if the process under control is open-loop unstable, failures in the plant-controller communication can result in environmental damages.

The concept of cyber-physical security mostly concerns security against malicious attacks. There are varieties of attacks such as *Denial-of-Service attacks, zero-dynamics attacks, bias injection attacks*, to name a few [3]. The last two are examples of attacks affecting the integrity of data, while Denial-of-Service attacks are meant to compromise the availability of data.

This paper is concerned with Denial-of-Service (DoS) attacks. We consider a sampled-data control system in which the measurement channel (sensor-to-controller channel) is networked; the attacker objective is to induce closed-loop instability by interrupting the plant-controller communication. In wireless networks, this can be caused by emitting intentional noise, also known as *jamming*, examples being constant, random and protocol-aware jamming [4]–[6]. It is generally accepted that communication failures induced by DoS can have a temporal profile quite different from the one exhibited by genuine packet losses, as assumed in the majority of studies on networked control; in particular, communication failures induced by DoS need not follow a given class of probability distributions [7]. This raises new theoretical challenges from the perspective of analysis as well as control design.

In the literature, several contributions have been proposed dealing with networked control under DoS. In [7], [8], the authors consider the problem of finding optimal control and attack strategies assuming a maximum number of jamming actions over a prescribed (finite) control horizon. A similar formulation is considered in [9], where the authors study zero-sum games between controllers and strategic jammers. In [10], [11], the authors consider DoS attacks in the form of pulse-width modulated signals. The goal is to identify salient features of the DoS signal such as maximum on/off cycle in order to suitably schedule the transmission times. For the case of periodic jamming (of unknown period and duration), identification schemes are proposed for de-synchronizing the transmission times from the DoS signal.

In [12], [13], a framework is introduced where no assumption is made regarding the DoS attack underlying strategy. A general attack model is considered that only constrains the attacker action in time by posing limitations on the *frequency* of DoS attacks and their *duration*. The main contribution is an explicit characterization of frequency and duration of the DoS attacks under which closed-loop stability can be preserved by means of state-feedback policies. Building on the results in [12], extensions have been considered dealing with dynamic controllers [14], nonlinear [15] and distributed [16] systems. Recently, a similar formulation has been adopted in the context of DoS-resilient event-triggered control [17]; see also [14].

From the perspective of securing robustness against DoS, static feedback has inherent limitations. In fact, using static feedback one generates control updates only when new measurements become available. Intuitively, this limitation can be overcome by considering dynamic controllers. In particular, a natural approach is to equip the control system with prediction capabilities so as reconstruct the missing measurements from available data during the DoS periods. Prompted by the above considerations, this paper discusses the design of predictor-based controllers in the context of DoS-resilient networked control. Inspired by recent results on finite-time state observers [18], [19], we focus the attention on impulsive-like predictors consisting of dynamical observers with measurements-triggered state resetting. Both analog and digital implementations are discussed, and compared.

While the idea of using predictor-based controllers is intuitive, the result is perhaps surprising. In fact, this paper

Shuai Feng and Pietro Tesi are with ENTEG, Faculty of Mathematics and Natural Sciences, University of Groningen, 9747 AG Groningen, The Netherlands s.feng@rug.nl, p.tesi@rug.nl.

shows that impulsive-like predictors make it possible to *maximize* the amount of DoS that one can tolerate for the class of DoS signals introduced in [12], [13].

The paper is organized as follows. In Section II, we describe the framework of interest, and outline the paper contribution. Section III presents the main results. We first design analog predictor-based controllers and discuss the conditions under which stability is guaranteed. Second, we design digital predictor-based controllers and characterize sampling rate of the digital device and stability conditions. In Section IV, an example is discussed. Section V ends the paper with concluding remarks and possible extensions to the present research.

A. Notation

We denote by $\mathbb{R}$ the set of reals. Given $\alpha \in \mathbb{R}$, we let $\mathbb{R}_{>\alpha}$ ($\mathbb{R}_{\geq\alpha}$) denote the set of reals greater than (greater than or equal to) α. We let $\mathbb{N}_0$ denote the set of nonnegative integers, $\mathbb{N}_0 := \{0, 1, \ldots\}$. The prime denotes transpose. Given a vector $v \in \mathbb{R}^n$, $\|v\|$ is its Euclidean norm. Given a matrix M, $\|M\|$ is its spectral norm. Given two sets A and B, we denote by $B\backslash A$ the relative complement of A in B, *i.e.*, the set of all elements belonging to B, but not to A. Given a measurable time function $f : \mathbb{R}_{\geq 0} \mapsto \mathbb{R}^n$ and a time interval $[0, t)$ we denote the $\mathcal{L}_\infty$ norm of $f(\cdot)$ on $[0, t)$ by $\|f_t\|_\infty := \sup_{s\in[0,t)}\|f(s)\|$. Given a measurable time function $f : \mathbb{R}_{\geq 0} \mapsto \mathbb{R}^n$ we say that f is bounded if its $\mathcal{L}_\infty$ norm is finite.

II. The framework

A. Process dynamics and network

The process to be controlled is given by

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) + d(t) \\ y(t) = x(t) + n(t) \\ x(0) = x_0 \end{cases} \tag{1}$$

where $t \in \mathbb{R}_{\geq 0}$; $x \in \mathbb{R}^n$ is the state, $u \in \mathbb{R}^m$ is the control input and $y \in \mathbb{R}^p$ is measurement vector; A and B are matrices of appropriate size with (A, B) is stabilizable; $d \in \mathbb{R}^n$ and $n \in \mathbb{R}^p$ are unknown (bounded) disturbance and noise signals, respectively.

We assume that the measurement channel is networked and subject to Denial-of-Service (DoS) status. The former implies that measurements are sent only at discrete time instants. Let $\{t_k\}_{k\in\mathbb{N}_0} = \{t_0, t_1, \ldots\}$ denote the sequence of transmission attempts. Throughout the paper, we assume for simplicity that the transmission attempts are carried out periodically with period Δ, *i.e.*,

$$t_{k+1} - t_k = \Delta, \quad k \in \mathbb{N}_0 \tag{2}$$

with $t_0 = 0$ by convention. The more general case of aperiodic transmission policies can be pursued along the lines of [13]. We refer to DoS as the phenomenon for which some transmission attempts may fail. In this paper, we do not distinguish between transmissions that fail due to channel unavailability (*e.g.*, caused by radio-frequency jammers in protocols employing carrier sensing as medium access policy) and transmissions that fail due to DoS-induced packet corruption.

We shall denote by $\{z_m\}_{m\in\mathbb{N}_0} = \{z_0, z_1, \ldots\}$, $z_0 \geq t_0$, the sequence of time instants at which samples of y are successfully transmitted.

B. Control objective

The objective is to design Δ and a controller $\mathcal{K}$, possibly dynamic, in such a way that the closed-loop stability is maintained despite the occurrence of DoS periods. In this paper, by closed-loop stability we mean that all the signals in the closed-loop system remain bounded for any initial condition x_0 and bounded noise and disturbance signals, and converge to zero in the event that noise and disturbance signals converge to zero.

C. Assumptions −Time-constrained DoS

Clearly, the problem in question does not have a solution if the DoS amount is allowed to be arbitrary. Following [13], we consider a general DoS model that constrains the attacker action in time by only posing limitations on the frequency of DoS attacks and their duration. Let $\{h_n\}_{n\in\mathbb{N}_0}$, $h_0 \geq 0$, denote the sequence of DoS *off/on* transitions, *i.e.*, the time instants at which DoS exhibits a transition from zero (transmissions are possible) to one (transmissions are not possible). Hence,

$$H_n := \{h_n\} \cup [h_n, h_n + \tau_n[\tag{3}$$

represents the n-th DoS time-interval, of a length $\tau_n \in \mathbb{R}_{\geq 0}$, over which the network is in DoS status. If $\tau_n = 0$, then H_n takes the form of a single pulse at h_n. Given $\tau, t \in \mathbb{R}_{\geq 0}$ with $t \geq \tau$, let $n(\tau, t)$ denote the number of DoS *off/on* transitions over $[\tau, t[$, and let

$$\Xi(\tau, t) := \bigcup_{n\in\mathbb{N}_0} H_n \bigcap [\tau, t] \tag{4}$$

denote the subset of $[\tau, t]$ where the network is in DoS status.

We make the following assumptions.

Assumption 1: (*DoS frequency*). There exist constants $\eta \in \mathbb{R}_{\geq 0}$ and $\tau_D \in \mathbb{R}_{>\Delta}$ such that

$$n(\tau, t) \leq \eta + \frac{t - \tau}{\tau_D} \tag{5}$$

for all $\tau, t \in \mathbb{R}_{\geq 0}$ with $t \geq \tau$. ∎

Assumption 2: (*DoS duration*). There exist constants $\kappa \in \mathbb{R}_{\geq 0}$ and $T \in \mathbb{R}_{>1}$ such that

$$|\Xi(\tau, t)| \leq \kappa + \frac{t - \tau}{T} \tag{6}$$

for all $\tau, t \in \mathbb{R}_{\geq 0}$ with $t \geq \tau$. ∎

Remark 1: The rationale behind Assumption 1 is that occasionally DoS can occur at a rate faster than Δ but the average interval between consecutive DoS triggering is greater than Δ. By (5), one may in fact have intervals where $h_{n+1} - h_n \leq \Delta$, hence intervals where $n(\tau, t)$ is greater than or equal to the maximum number $\lceil (t - \tau)/\Delta \rceil$ of transmission attempts that may occur within $[\tau, t[$. However,

over large time windows, *i.e.*, when the term $(t-\tau)/\tau_D$ is predominant compared to η, the number of DoS triggering is at most of the order of $(t-\tau)/\tau_D$. Assumption 2 expresses a similar requirement with respect to the DoS duration. In fact, it expresses the property that, on the average, the time instants over which communication is interrupted do not exceed a certain *fraction* of time, as specified by the constant $T \in \mathbb{R}_{>1}$. Similarly to η, the constant $\kappa \in \mathbb{R}_{\geq 0}$ plays the role of a regularization term. It is needed because during a DoS interval, one has $|\Xi(h_n, h_n+\tau_n)| = \tau_n > \tau_n/T$ since $T > 1$. Accordingly, κ serves to make (6) consistent. Assumptions 1 and 2 are general enough to capture many different types of DoS attacks, including *trivial, periodic, random* and *protocol-aware jamming* attacks [5], [6]; see [13] for a more detailed discussion. ∎

Remark 2: Unless other conditions are imposed, both the requirements $\tau_D > \Delta$ and $T > 1$ are necessary in order for the stabilization problem to be well-posed. In fact, if $\tau_D = \Delta$ then the DoS signal characterized by the pair $(h_n, \tau_n) = (t_k, 0)$ satisfies Assumptions 1 and 2 with $\eta = 1$, $\kappa = 0$ and $T = \infty$ but destroys any communication attempt. Likewise, in case $T = 1$ then the DoS signal characterized by $(h_0, \tau_0) = (0, \infty)$ satisfies Assumptions 1 and 2 with $\eta = 1$, $\kappa = 0$ and $\tau_D = \infty$ but destroys any communication attempt. ∎

D. Previous work and paper contribution

In [13], the problem of achieving robustness against DoS has been analyzed for the case of static feedback laws

$$u(t) = \begin{cases} 0, & t \in [0, z_0[\\ Ky(z_m), & t \in [z_m, z_{m+1}[,\ m \in \mathbb{N}_0 \end{cases} \tag{7}$$

where K is a state-feedback matrix designed in such a way that all the eigenvalues of $\Phi = A + BK$ have negative real part. For this scenario, a characterization of stabilizing transmission policies was given. We summarize below this result.

Theorem 1: Consider the process (1) under a control action as in (7). Given any positive definite symmetric matrix Q, let P denote the solution of the Lyapunov equation $\Phi' P + P\Phi + Q = 0$. Let the transmission policy in (2) be such that

$$\Delta \leq \frac{1}{\mu_A} \log \left[\left(\frac{\sigma}{1+\sigma} \right) \frac{1}{\max\{\|\Phi\|, 1\}} \mu_A + 1 \right] \tag{8}$$

when $\mu_A > 0$, and

$$\Delta \leq \left(\frac{\sigma}{1+\sigma} \right) \frac{1}{\max\{\|\Phi\|, 1\}} \tag{9}$$

when $\mu_A \leq 0$, where μ_A is the logarithmic norm of A and σ is a positive constant satisfying $\gamma_1 - \sigma\gamma_2 > 0$, where γ_1 is equal to the smallest eigenvalue of Q and $\gamma_2 := \|2PBK\|$. Then, the closed-loop system is stable for any DoS sequence satisfying Assumption 1 and 2 with arbitrary η and κ, and with τ_D and T such that

$$\frac{1}{T} + \frac{\Delta}{\tau_D} < \frac{\omega_1}{\omega_1 + \omega_2} \tag{10}$$

where $\omega_1 := (\gamma_1 - \gamma_2\sigma)/2\alpha_2$ and $\omega_2 := 2\gamma_2/\alpha_1$, where α_1 and α_2 denote the smallest and largest eigenvalue of P, respectively. ∎

Inequality (10) provides an explicit characterization of the robustness degree against DoS that static feedback policies can achieve. This characterization relates the DoS parameters τ_D and T with the transmission period Δ and the control system parameters via ω_1 and ω_2, which depend on choice of the state-feedback matrix K.

Clearly, increasing the right-hand side of (10) increases the amount of DoS that the control system can tolerate. However, with static feedback it is difficult to obtain large values for the right-hand side of (10). The underlying reason is that static feedback has the inherent limitation of generating control updates only when new measurements become available, and this possibly reflects in small values for the right-hand side of (10). Intuitively, this limitation can be overcome by equipping the controller with prediction capabilities, with the idea of compensating DoS by reconstructing the missing measurements from available data. In the next section, it is shown that using predictor-based controllers one can achieve closed-loop stability whenever

$$\frac{1}{T} + \frac{\Delta}{\tau_D} < 1 \tag{11}$$

holds true.

While the idea of using predictor-based controllers is intuitive, the result is perhaps surprising. In fact, this is the best possible bound that one can achieve for DoS signals satisfying Assumption 1 and 2. Indeed, if we denote by $\mathcal{S}(\tau_D, T)$ the class of DoS signals for which (11) is not satisfied, then $\mathcal{S}(\tau_D, T)$ does always contain DoS signals for which stability is destroyed. Examples are DoS signals characterized by $(\tau_D, T) = (\Delta, \infty)$ and $(\tau_D, T) = (\infty, 1)$; *cf.* Remark 2.

III. Main results

In Section III-A, we discuss one technical result which is fundamental for the developments of the paper. The theoretical analysis for analog predictor-based controllers is presented in Section III-B, while in Section III-C we will further extend our work to digital implementations.

A. Key lemma

The following lemma relates DoS parameters and time elapsing between successful transmissions.

Lemma 1: Consider a transmission policy as in (2), along with a DoS signal satisfying Assumption 1 and 2. If (11) holds true, then the sequence of successful transmissions satisfies $z_0 \leq Q$ and $z_{m+1} - z_m \leq Q + \Delta$ for all $m \in \mathbb{N}_0$, where

$$Q = (\kappa + \eta\Delta) \left(1 - \frac{1}{T} - \frac{\Delta}{\tau_D} \right)^{-1} \tag{12}$$

Proof. We first define some auxiliary quantities. Let $\bar{H}_n := \{h_n\} \cup [h_n, h_n + \tau_n + \Delta[$ represent the n-th DoS interval prolonged by one sampling. For any interval $[\tau, t]$,

let $\bar{\Xi}(\tau,t) := \bigcup_{n\in\mathbb{N}_0} \bar{H}_n \bigcap [\tau,t]$ and $\bar{\Theta}(\tau,t) := [\tau,t]\backslash\bar{\Xi}(\tau,t)$. The main idea for the proof relies on the following argument. Given h_n, we have

$$\begin{aligned} |\bar{\Theta}(h_n,t)| &= t - h_n - |\bar{\Xi}(h_n,t)| \\ &\geq t - h_n - |\Xi(h_n,t)| - n(h_n,t)\Delta \\ &\geq (t-h_n)\left(1 - \frac{1}{T} - \frac{\Delta}{\tau_D}\right) - \kappa - \eta\Delta \end{aligned} \quad (13)$$

for all $t \geq h_n$ where the first inequality follows from the definition of the set $\bar{\Xi}(\tau,t)$ while the second inequality follows from Assumption 1 and 2. Notice that $|\bar{\Theta}(h_n,t)| > 0$ implies that $[h_n,t]$ contains at least one successful transmission. This is because $|\bar{\Theta}(h_n,t)| > 0$ implies that $[h_n,t]$ contains a DoS-free interval of length greater than Δ. We claim that a successful transmission does always occur within $[h_n, h_n+Q]$. To this end, suppose that the claim is false and let t_* denote the last transmission attempt occurring within $[h_n, h_n+Q]$. Since t_* is unsuccessful $|\bar{\Theta}(h_n,t_*)| = 0$. Moreover, this also implies $|\bar{\Theta}(h_n,t_*+\Delta)| = 0$. This is because, if t_* is unsuccessful then it must be contained in a DoS interval, say H_q, so that $[t_*,t_*+\Delta[\subseteq \bar{H}_q$. However, since $t_*+\Delta > h_n+Q$ we also have

$$\begin{aligned} &|\bar{\Theta}(h_n,t_*+\Delta)| \\ &\qquad > Q\left(1-\frac{1}{T}-\frac{\Delta}{\tau_D}\right) - \kappa - \eta\Delta = 0 \end{aligned}$$

which leads to a contradiction.

Based on these arguments, the proof can be readily finalized. Consider first $z_0 \leq Q$. If t_0 is successful then the claim holds trivially. Suppose instead that t_0 is unsuccessful, *i.e.*, $h_0 = 0$. By the above arguments we have one successful transmission no later than h_0+Q and, hence, no later than Q. Consider next $z_{m+1} - z_m \leq Q+\Delta$. If $z_m+\Delta$ is successful, then the claim holds trivially. Suppose instead that $z_m+\Delta$ is unsuccessful. Since z_m is successful a DoS must occur within $]z_m, z_m+\Delta]$. Hence, we must have $h_n \in]z_m, z_m+\Delta]$ for some $n \in \mathbb{N}_0$. By the above arguments we have one successful transmission no later than h_n+Q and, hence, no later than $z_m+Q+\Delta$. ∎

Remark 3: In the absence of DoS, when $T = \tau_D = \infty$ and $\kappa = \eta = 0$, Q becomes zero. In fact, in the absence of DoS, Lemma 1 simply describes the functioning of a standard periodic transmission policy. ∎

B. Analog predictor-based controller

The considered predictor-based controller consists of two parts: prediction and state-feedback. As for the prediction part, we consider an impulsive predictor, whose dynamics are given by

$$\begin{cases} \dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t), & t \neq z_m \\ \hat{x}(t) = y(t), & t = z_m \end{cases} \quad (14)$$

with initial condition

$$\hat{x}(0) = \begin{cases} y(0), & \text{if } z_0 = 0 \\ 0, & \text{otherwise} \end{cases} \quad (15)$$

where $t \in \mathbb{R}_{\geq 0}$ and $m \in \mathbb{N}_0$. By construction the solution $\hat{x}$ is continuous from the right everywhere.

The state-feedback matrix is an arbitrary matrix K such that all the eigenvalues of $\Phi = A + BK$ have negative real part. Then, the control input applied to the process (and the predictor) is given by

$$u(t) = K\hat{x}(t) \quad (16)$$

where $t \in \mathbb{R}_{\geq 0}$.

The predictor differs from a classical asymptotic observer due to the measurements-triggered jumps in the state. The reason for considering an impulsive-like predictor rather than an asymptotic one is the following. Let

$$e(t) := \hat{x}(t) - x(t) \quad (17)$$

where $t \in \mathbb{R}_{\geq 0}$. The process dynamics can be therefore expressed as

$$\dot{x}(t) = \Phi x(t) + BKe(t) + d(t) \quad (18)$$

where $t \in \mathbb{R}_{\geq 0}$. Consider any symmetric positive definite matrix Q, and let P be the solution of the Lyapunov equation $\Phi' P + P\Phi + Q = 0$. Let $V(x) = x'Px$. Its derivative along the solutions to (18), satisfies

$$\begin{aligned} \dot{V}(x(t)) \leq &- \gamma_1 \|x(t)\|^2 + \gamma_2 \|x(t)\| \|e(t)\| \\ &+ \gamma_3 \|x(t)\| \|d(t)\| \end{aligned} \quad (19)$$

for all $t \in \mathbb{R}_{\geq 0}$, where γ_1 is the smallest eigenvalue of Q, $\gamma_2 := \|2PBK\|$ and $\gamma_3 := \|2P\|$. From the last expression one sees that stability depends on the magnitude of e. In this respect, the dynamics of e obeys

$$\begin{aligned} \dot{e}(t) &= Ae(t) - d(t), \quad t \neq z_m \\ e(t) &= n(t), \quad t = z_m \end{aligned} \quad (20)$$

where $t \in \mathbb{R}_{\geq 0}$ and $m \in \mathbb{N}_0$. One sees from the second equation of (20) that resetting the predictor state makes it possible to reset e to a bounded value whenever a new measurement becomes available. In turns, Lemma 1 ensures that a resetting does always occur in a finite time. These two properties guarantee boundedness of e for all $t \geq z_0$.

In particular, we have the following result.

Lemma 2: Consider the process (1) with predictor-based controller (14)-(16) under a transmission policy as in (2). Consider any DoS sequence satisfying Assumption 1 and 2 with arbitrary η and κ, and with τ_D and T satisfying (11). Then, there exists a positive constant ρ such that

$$\|e(t)\| \leq \rho \|w_t\|_\infty \quad (21)$$

for all $t \in \mathbb{R}_{\geq z_0}$, where $w = [d' \; n']'$.

Proof. Consider any interval $[z_m, z_{m+1}[$, $m \in \mathbb{N}_0$. By (20), we have

$$e(t) = e^{A(t-z_m)} n(z_m) - \int_{z_m}^{t} e^{A(t-\tau)} d(\tau) d\tau \quad (22)$$

for all $t \in [z_m, z_{m+1}[$.

Let now μ_A denote the logarithmic norm of A. If $\mu_A \leq 0$, we obtain

$$\begin{aligned}\|e(t)\| &\leq \|n(z_m)\| + \|d_t\|_\infty (t - z_m) \\ &\leq \|n_t\|_\infty + \|d_t\|_\infty (Q + \Delta)\end{aligned} \tag{23}$$

for all $t \in [z_m, z_{m+1}[$, where the second inequality follows from Lemma 1. If instead $\mu_A > 0$, we have

$$\begin{aligned}\|e(t)\| &\leq e^{\mu_A (t - z_m)} \|n(z_m)\| + \frac{1}{\mu_A} \left(e^{\mu_A (t - z_m)} - 1 \right) \|d_t\|_\infty \\ &\leq e^{\mu_A (Q + \Delta)} \|n_t\|_\infty + \frac{1}{\mu_A} \left(e^{\mu_A (Q + \Delta)} - 1 \right) \|d_t\|_\infty\end{aligned} \tag{24}$$

where the second inequality follows again from Lemma 1. Hence, we conclude that the claim holds with

$$\rho := 1 + Q + \Delta \tag{25}$$

if $\mu_A \leq 0$, and with

$$\rho := \left(1 + \frac{1}{\mu_A} \right) e^{\mu_A (Q + \Delta)} \tag{26}$$

if $\mu_A > 0$. ∎

Exploiting Lemma 2, we obtain the following stability result for analog controller implementations.

Theorem 2: Consider the process (1) with predictor-based controller (14)-(16) under a transmission policy as in (2). Then, the closed-loop system is stable for any DoS sequence satisfying Assumption 1 and 2 with arbitrary η and κ, and with τ_D and T satisfying (11).

Proof. Consider the closed-loop dynamics for all $t \geq z_0$. Notice that z_0 exists finite by virtue of Lemma 1. In view of (19) and Lemma 2, we have

$$\dot{V}(x(t)) \leq -\gamma_1 \|x(t)\|^2 + \gamma_4 \|x(t)\| \|w_t\|_\infty \tag{27}$$

for all $t \in \mathbb{R}_{\geq z_0}$, where $\gamma_4 := \gamma_2 \rho + \gamma_3$.

Observe that for any positive real β, the Young's inequality yields

$$2\|x(t)\| \|w_t\|_\infty \leq \frac{1}{\beta} \|x(t)\|^2 + \beta \|w_t\|_\infty \tag{28}$$

Using this inequality with $\beta = \gamma_4 / \gamma_1$, straightforward calculations yield

$$\dot{V}(x(t)) \leq -\omega_1 V(x(t)) + \gamma_5 \|w_t\|_\infty^2 \tag{29}$$

for all $t \in \mathbb{R}_{\geq z_0}$, where $\omega_1 := \gamma_1 / (2\alpha_2)$ and $\gamma_5 := \gamma_4^2 / (2\gamma_1)$, where α_2 denotes the largest eigenvalue of P. Accordingly, we obtain

$$V(x(t)) \leq e^{-\omega_1 (t - z_0)} V(x(z_0))) + \frac{\gamma_5}{\omega_1} \|w_t\|_\infty^2 \tag{30}$$

for all $t \in \mathbb{R}_{\geq z_0}$. This shows that x remains bounded because z_0 exists finite in view of Lemma 1. In turns, this implies that also $\hat{x}$ remains bounded. Moreover, in the event that disturbance and noise signals converge to zero, (20) implies that e converges to zero. In turns, (19) implies that both x and $\hat{x}$ also converge to zero. ∎

Remark 4: The considered controller yields quite strong stability properties, namely global exponential stability with linear bounds on the map from the disturbance and noise signals to the process state. It is also interesting to observe that, as long as the triplet (τ_D, T, Δ) satisfies (11), Δ can be chosen arbitrarily (though large values of Δ may affect the performance via γ_5, which depends on ρ). In particular, in the absence of DoS when $T = \tau_D = \infty$ and $\kappa = \eta = 0$, then (11) is satisfied for any bounded value of Δ. This is due to the controller state resetting mechanism. ∎

C. Digital predictor-based controller

In this section, we extend the control algorithm to a digital implementation. The substantial difference between analog and digital implementations is that in the latter the control action can be updated only at a finite rate. Because of this, Lemma 2 does not hold any longer. As we will see, in order to recover a boundedness inequality similar to the one in Lemma 2, constraints have to be enforced on the sampling rate of the digital controller.

Consider a digital controller with sampling rate

$$\delta = \frac{\Delta}{b} \tag{31}$$

where b is any positive integer. Choosing the controller sampling rate as a submultiple of Δ makes it possible to implement the controller as a sampled-data version of (14), which is synchronized with the network transmission rate. Let $A_\delta = e^{A\delta}$ and $B_\delta = \int_0^\delta e^{A\tau} B d\tau$. The digital predictor is given by

$$\begin{cases} \hat{x}((q+1)\delta) = A_\delta \alpha(q\delta) + B_\delta u(q\delta) \\ \alpha(q\delta) = \begin{cases} y(q\delta), & \text{if } q\delta = z_m \\ \hat{x}(q\delta), & \text{otherwise} \end{cases} \\ \hat{x}(0) = 0 \end{cases} \tag{32}$$

where $q \in \mathbb{N}_0$.

The control action is given by

$$u(q\delta) = K \alpha(q\delta). \tag{33}$$

where $q \in \mathbb{N}_0$.

Similar to the analog implementation, also the digital implementation is equipped with a state resetting mechanism. Due to the discrete nature of the update equations, the resetting mechanism is implemented using an auxiliary variable α.

The stability analysis follows the same steps as in the previous case. Let

$$\phi(t) := \alpha(q\delta) - x(t) \tag{34}$$

where $t \in I_q := [q\delta, (q+1)\delta[$, $q \in \mathbb{N}_0$. Hence, the process dynamics satisfies

$$\dot{x}(t) = \Phi x(t) + BK\phi(t) + d(t) \tag{35}$$

for all $t \in I_q$.

Given any symmetric positive definite matrix Q, let P be the solution of the Lyapunov equation $\Phi' P + P\Phi + Q = 0$. Let $V(x) = x'Px$. Its derivative along the solutions to (35), satisfies

$$\begin{aligned}\dot{V}(x(t)) \leq & -\gamma_1 \|x(t)\|^2 + \gamma_2 \|x(t)\| \|\phi(t)\| \\ & + \gamma_3 \|x(t)\| \|d(t)\| \end{aligned} \tag{36}$$

for all $t \in I_q$, where γ_1 is the smallest eigenvalue of Q, $\gamma_2 := \|2PBK\|$ and $\gamma_3 := \|2P\|$. As in the previous case, stability depends on the magnitude of ϕ. In this respect, the dynamics of ϕ satisfies

$$\begin{aligned}\dot{\phi}(t) &= -\dot{x}(t) \\ &= A\phi(t) - \Phi\alpha(q\delta) - d(t), \quad t \neq z_m \\ \phi(t) &= n(t), \quad t = z_m \end{aligned} \tag{37}$$

for all $t \in I_q$.

The differential equation in (37) differs from its analog counterpart in (20) due to the extra term $\Phi\alpha(q\delta)$. Because of this, Lemma 2 breaks down. In order to recover a property similar to the one established in Lemma 2, constraints have to be enforced on the sampling rate of the digital controller. This is consistent with intuition, and simply indicates that the rate of control updates has to be sufficiently fast. In this respect, letting $\delta = \Delta/b$ allows to differentiate between controller sampling rate and transmission rate, maintaining Δ possibly large.

Lemma 3: Consider the process (1) with predictor-based controller (32)-(33) under a transmission policy as in (2). Consider any DoS sequence satisfying Assumption 1 and 2 with arbitrary η and κ, and with τ_D and T satisfying (11). Let the controller sampling rate be such that

$$\delta \leq \frac{1}{\mu_A} \log \left[\left(\frac{\sigma}{1+\sigma} \right) \frac{1}{\max\{\|\Phi\|, 1\}} \mu_A + 1 \right] \tag{38}$$

when $\mu_A > 0$, and

$$\delta \leq \left(\frac{\sigma}{1+\sigma} \right) \frac{1}{\max\{\|\Phi\|, 1\}} \tag{39}$$

when $\mu_A \leq 0$, where μ_A is the logarithmic norm of A and σ is a positive constant satisfying $\gamma_1 - \sigma\gamma_2 > 0$, where γ_1 is equal to the smallest eigenvalue of Q and $\gamma_2 := \|2PBK\|$. Then, there exists a positive constant $\tilde{\rho}$ such that

$$\|\phi(t)\| \leq \sigma \|x(t)\| + \tilde{\rho} \|w_t\|_\infty \tag{40}$$

for all $t \in \mathbb{R}_{\geq z_0}$.

Proof. Consider any interval $[z_m, z_{m+1}[$, $m \in \mathbb{N}_0$, and any controller sampling instant $q\delta \in [z_m, z_{m+1}[$. The proof is divided into two steps. In the first step, we provide an upper bound on the error dynamics ϕ at the controller sampling time $q\delta$. Second, we provide an upper bound on the error dynamics ϕ between controller inter-samplings. In turns, this provides an upper bound on ϕ over the whole interval $[z_m, z_{m+1}[$, and, hence, over $\mathbb{R}_{\geq z_0}$.

For the sake of convenience, we will relate a controller update instant $q\delta$ with a successful transmission instant z_m via the expression

$$q\delta = z_m + p\delta \tag{41}$$

where $p \in \mathbb{N}_0$. This is always possible since $\delta = \Delta/b$.

We start by deriving an upper bound on $\phi(q\delta)$. It is simple to verify that the dynamics of the variable α in the controller equations satisfies

$$\begin{aligned}\alpha(q\delta) = & A_\delta^p \, \alpha(z_m) \\ & + \sum_{k=0}^{p-1} A_\delta^{p-k-1} B_\delta \, u(z_m + k\delta) \end{aligned} \tag{42}$$

In fact, between two successful transmissions, α coincides with $\hat{x}$, which evolves like a classical linear time-invariant discrete-time system.

On the other hand,

$$\begin{aligned}x(t) = & \, e^{A(t-z_m)} x(z_m) + \int_{z_m}^{t} e^{A(t-\tau)} B u(\tau) d\tau \\ & + \int_{z_m}^{t} e^{A(t-\tau)} d(\tau) d\tau \end{aligned} \tag{43}$$

for all $t \in [z_m, z_{m+1}[$.

Combining the two expressions, we get

$$\begin{aligned}\phi(q\delta) &= \alpha(q\delta) - x(q\delta) \\ &= e^{A(q\delta - z_m)} n(z_m) - \int_{z_m}^{q\delta} e^{A(q\delta-\tau)} d(\tau) d\tau \end{aligned} \tag{44}$$

where we exploited the relation $A_\delta^p = e^{Ap\delta} = e^{A(q\delta - z_m)}$, and the fact that

$$\begin{aligned}&\int_{z_m}^{q\delta} e^{A(q\delta-\tau)} B u(\tau) d\tau \\ &= \sum_{k=0}^{p-1} \left[\int_{z_m+k\delta}^{z_m+(k+1)\delta} e^{A(q\delta-\tau)} B d\tau \right] u(z_m + k\delta) \\ &= \sum_{k=0}^{p-1} e^{A\delta(p-k-1)} \left[\int_0^{\delta} e^{As} B ds \right] u(z_m + k\delta) \\ &= \sum_{k=0}^{p-1} A_\delta^{p-k-1} B_\delta u(z_m + k\delta) \end{aligned} \tag{45}$$

where the second equality is obtained using the change of variable $s = z_m + (k+1)\delta - \tau$.

We can now obtain an upper bound on $\phi(q\delta)$. Specifically, since by hypothesis $q\delta \in [z_m, z_{m+1}[$, we have

$$\|\phi(q\delta)\| \leq \rho \|w_{q\delta}\|_\infty \tag{46}$$

where ρ is defined as in Lemma 2.

We can now provide an upper bound on ϕ between controller inter-samplings. Let

$$f(t - q\delta) := \int_{q\delta}^{t} e^{A(t-\tau)} d\tau \tag{47}$$

Integrating (37) over the interval I_q, we obtain

$$\begin{aligned}\|\phi(t)\| &\leq \|e^{A(t-q\delta)}\|\|\phi(q\delta)\| \\ &\quad + f(t-q\delta)\|d_t\|_\infty + f(t-q\delta)\|\Phi\|\|\alpha(q\delta)\| \\ &\leq \hat{\rho}\,\rho\|w_t\|_\infty \\ &\quad + f(t-q\delta)\|d_t\|_\infty + f(t-q\delta)\|\Phi\|\|\alpha(q\delta)\| \\ &\leq \hat{\rho}\,\rho\|w_t\|_\infty \\ &\quad + f(t-q\delta)\|d_t\|_\infty \\ &\quad + f(t-q\delta)\|\Phi\|(\|\phi(t)\| + \|x(t)\|) \end{aligned} \tag{48}$$

for all $t \in I_q$, where $\hat{\rho} := \max\{e^{\mu_A \delta}, 1\}$.

Let $\kappa_1 := \max\{\|\Phi\|, 1\}$. Observe that $f(0) = 0$ and that $f(t - q\delta)$ is monotonically increasing with t. Accordingly, any positive real δ such that

$$f(\delta) \leq \frac{1}{\kappa_1}\frac{\sigma}{(1+\sigma)}, \tag{49}$$

ensures (40) with

$$\tilde{\rho} := \sigma + \hat{\rho}\rho(1+\sigma) \tag{50}$$

We finally derive an explicit expression for δ. If $\mu_A > 0$, we have

$$f(\delta) = \frac{1}{\mu_A}(e^{\mu_A \delta} - 1) \tag{51}$$

and (38) yields the desired result. If instead $\mu_A \leq 0$, then $f(\delta) \leq \delta$, and (39) yields the desired result.

This concludes the proof. ∎

Based on Lemma 3 the following result can be stated, which provides a natural counterpart of Theorem 2.

Theorem 3: Consider the process (1) with predictor-based controller (32)-(33) under a transmission policy as in (2). Let the controller sampling rate be chosen as in Lemma 3. Then, the closed-loop system is stable for any DoS sequence satisfying Assumption 1 and 2 with arbitrary η and κ, and with τ_D and T satisfying (11).

Proof. Consider the closed-loop dynamics for all $t \geq z_0$. Substituting (40) into (36) yields

$$\begin{aligned}\dot{V}(x(t)) \leq\ & -(\gamma_1 - \sigma\gamma_2)\|x(t)\|^2 \\ & +(\gamma_2\tilde{\rho} + \gamma_3)\|x(t)\|\|w_t\|_\infty \end{aligned} \tag{52}$$

for all $t \in \mathbb{R}_{z_0}$, where $\gamma_1 - \sigma\gamma_2$ is strictly positive by construction. The conclusion is that the proof Theorem 2 carries over to Theorem 3 with γ_1 and γ_4 replaced by $\gamma_1 - \sigma\gamma_2$ and $\gamma_2\tilde{\rho} + \gamma_3$, respectively. ∎

Compared with the analog implementation, one sees that the digital implementation does only require a proper choice of the controller sampling rate. On the other hand, it achieves the same robustness properties of the analog implementation. By Lemma 3, admissible values for the controller sampling rate can be explicitly computed from the parameters of the control system.

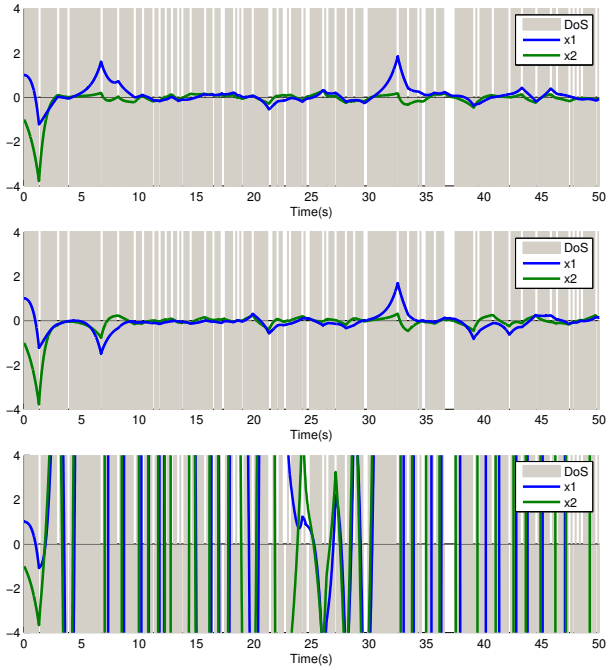

Fig. 1. Simulation results for the example. Top: Analog controller; Center: Digital Controller; Bottom: Pure static feedback.

IV. Example

The numerical example is taken from [20]. The system to be controlled is open-loop unstable and is characterized by the matrices

$$A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \quad B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{53}$$

The state-feedback matrix is given by

$$K = \begin{bmatrix} -2.1961 & -0.7545 \\ -0.7545 & -2.7146 \end{bmatrix} \tag{54}$$

The control system parameters are $\gamma_1 = 1$, $\gamma_2 = 2.1080$, $\alpha_1 = 0.2779$, $\alpha_2 = 0.4497$, $\|\Phi\| = 1.9021$ and $\mu_A = 1.5$. Disturbance d and noise n are random signals with uniform distribution in $[-0.1, 0.1]$.

The network transmission rate is given by $\Delta = 0.1$s. Both analog and digital controllers are considered. As for the digital implementation, in accordance with Lemma 3, we must select σ such that $\sigma < 0.4744$. According to (38), we obtain the constraint $\delta < 0.1508$. We select $\delta = 0.01$s so that δ is sufficiently small, and in order to synchronize the controller sampling rate with Δ.

Figure 1 shows simulation results, which compare the static feedback law (7) with the predictor-based controllers (14)-(16) and (32)-(33). We consider a sustained DoS attack with variable period and duty cycle, generated randomly. Over a simulation horizon of 50s, the DoS signal yields $|\Xi(0, 50)| = 38.8$s and $n(0, 50) = 52$. This corresponds to values (averaged over 50s) of $\tau_D \approx 0.96$ and $T \approx 1.29$, and $\sim 80\%$ of transmission failures. For the predictor-based

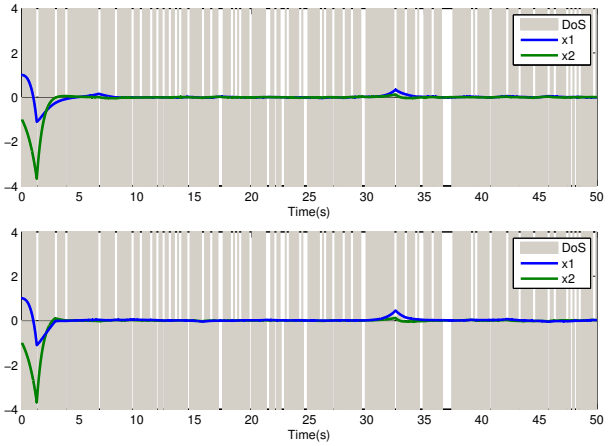

Fig. 2. Simulation results for the example in case disturbance and noise are random signals with uniform distribution in $[-0.01, 0.01]$. Top: Analog controller; Bottom: Digital Controller.

controllers, the stability requirement is satisfied since

$$\frac{\Delta}{\tau_D} + \frac{1}{T} \approx 0.8793 \tag{55}$$

On the other hand, the DoS parameters do not satisfy the stability requirement for the pure static feedback law, which is (*cf.* (10))

$$\frac{\Delta}{\tau_D} + \frac{1}{T} < 0.0321 \tag{56}$$

The theoretical bound for the case of pure static feedback is conservative (indeed, simulations show that (7) ensures closed-loop stability for the system in (53) up to $\sim 40\%$ of transmission failures). Nonetheless, the improvement given by predictor-based controllers is significant. In fact, while the system undergoes instability with (7), the performance level provided by (14)-(16) and (32)-(33) is very high despite the sustained DoS attack.

It is worth noting that while stability is independent on the magnitude of disturbance and noise signals, performance is not. As shown in Figure 2, noise significantly impacts on the accuracy of the state estimate, and, hence, on the closed-loop behavior during DoS status; *cf.* the paper conclusions.

V. Concluding remarks

In this paper, we investigated the problem of designing DoS-resilient control systems. It was shown that the use of dynamical observers with state resetting mechanism makes it possible to maximize the amount of DoS that one can tolerate for a general class of DoS signals. Both analog and digital implementations have been discussed, the latter requiring a suitable choice of the controller sampling rate.

The results presented in this paper can be extended in various directions. We envision the use of a similar control architecture for the case of partial state measurements, via the approach considered in [18]. Another interesting study concerns performance robustness against measurement noise, which is the main factor affecting the quality of the process state estimation. The recent results in [21] may prove relevant in this regard.

References

[1] E. Lee, "Cyber physical systems: Design challenges," in *2008 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing (ISORC)*, 2008, pp. 363–369.

[2] L. Sha, S. Gopalakrishnan, L. Xue, and W. Qixin, "Cyber physical systems: A new frontier," in *IEEE International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing, 2008. SUTC '08*, 2008, pp. 1–9.

[3] A. Teixeira, I. Shames, H. Sandberg, and K. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.

[4] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *Communications Surveys & Tutorials, IEEE*, vol. 13, no. 2, pp. 245–257, 2011.

[5] P. Tague, M. Li, and R. Poovendran, "Mitigation of control channel jamming under node capture attacks," *IEEE Transactions on Mobile Computing*, vol. 8, no. 9, pp. 1221–1234, 2009.

[6] B. DeBruhl and P. Tague, "Digital filter design for jamming mitigation in 802.15. 4 communication," in *Computer Communications and Networks (ICCCN), 2011 Proceedings of 20th International Conference on*, 2011, pp. 1–6.

[7] S. Amin, A. Càrdenas, and S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," *Hybrid systems: Computation and Control*, pp. 31–45, 2009.

[8] A. Gupta, C. Langbort, and T. Başar, "Optimal control in the presence of an intelligent jammer with limited actions," in *Proc. of the 49th IEEE Conference on Decision and Control, Atlanta, GA, USA*, 2010, pp. 1096–1101.

[9] V. Ugrinovskii and C. Langbort, "Control over adversarial packet-dropping communication networks revisited," *arXiv:1403.5641*, 2014.

[10] H. Shisheh Foroush and S. Martínez, "On event-triggered control of linear systems under periodic denial of service attacks," in *Proc. of the IEEE Conference on Decision and Control, Maui, HI, USA*, 2012, pp. 2551–2556.

[11] ——, "On multi-input controllable linear systems under unknown periodic dos jamming attacks," in *2013 SIAM Conference on Control and its Applications, San Diego, CA*, 2013.

[12] C. De Persis and P. Tesi, "Resilient control under denial-of-service," in *Proc. of the 19th IFAC World Conference, Cape Town, South Africa*, 2014, pp. 134–139.

[13] C. D. Persis and P. Tesi, "Input-to-state stabilizing control under denial-of-service," *IEEE Transactions on Automatic Control*, vol. 60, no. 11, pp. 2930–2944, 2015.

[14] V. Dolk, P. Tesi, C. De Persis, and W. Heemels, "Event-triggered control systems under denial-of-service attacks," in *Proc. of the 54th IEEE Conference on Decision and Control, Osaka, Japan*, 2015.

[15] C. De Persis and P. Tesi, "On resilient control of nonlinear systems under denial-of-service," in *Proc. of the IEEE Conference on Decision and Control, Los Angeles, CA, USA*, 2014.

[16] D. Senejohnny, P. Tesi, and C. De Persis, "Self-triggered coordination over a shared network under denial-of-service," in *Proc. of the 54th IEEE Conference on Decision and Control, Osaka, Japan*, 2015.

[17] A. Cetinkaya, H. Ishii, and T. Hayakawa, "Event-triggered control over unreliable networks subject to jamming attacks," *arXiv:1403.5641*, 2015.

[18] T. Raff and F. Allgöwer, "An observer that converges in finite time due to measurement-based state updates," in *Proc. of the 17th IFAC World Conference, Seoul, South Korea*, 2008, pp. 2693–2695.

[19] F. Ferrante, F. Gouaisbaut, R. Sanfelice, and S. Tarbouriech, "An observer with measurement-triggered jumps for linear systems with known input," in *Proc. of the 19th IFAC World Conference, Cape Town, South Africa*, 2014, pp. 140–145.

[20] F. Forni, S. Galeani, D. Nešić, and L. Zaccarian, "Lazy sensors for the scheduling of measurement samples transmission in linear closed loops over networks," in *IEEE Conference on Decision and Control and European Control Conference, Atlanta, USA*, 2010.

[21] Y. Li and R. Sanfelice, "A finite-time convergent observer with robustness to piecewise-constant measurement noise," *Automatica*, vol. 57, pp. 222–230, 2015.